W.P. & T.Div. 1st Memo Ind. aln

War Plans & Training Div., OCSigO, March 30, 1932 - To C.I.C., Research and Development Division, OCSigO.

I concur in Paragraphs 7, 8 and 9, basic memorandum.

D. M. Crawford,
Major, Signal Corps.

WAR DEPARTMENT
aln
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

March 29, 1932

MEMORANDUM TO: Executive Officer (THROUGH O.I.C. War Plans and Training Division and O.I.C. Research and Development Division).

1. This report deals with my visit to the Signal Corps Laboratories, March 21 - 24, 1932.

2. Immediately after arrival, Monday afternoon, and after reporting at headquarters, Fort Monmouth, I had a conference with Mr. Graham in regard to the cipher facsimile system of the German inventor, Dr. Wrede, for the purpose of discussing the outlines of the conference to be held with the inventor the next day, Tuesday. A copy of the report written by Mr. Graham and myself, and the conclusions reached in regard to the Wrede system, after full discussions with Dr. Wrede on Tuesday, will be submitted later.

3. Wednesday was devoted to discussions with Mr. Graham and his assistants while the various elements of the Signal Corps cipher machine being constructed at the laboratories were being assembled for the first time. In the late afternoon the machine was completely assembled, in working order, and made ready for a preliminary test, Thursday morning. Some minor difficulties were encountered, occasioned by the fact that one of the control relays apparently did not operate with sufficient speed to accomplish its function. On Thursday morning I prepared a plain-text message of 500 letters and proceeded to encipher it by the machine. This test required twenty minutes, the machine operating in a very satisfactory manner at the rate of twenty-five letters per minute.

4. The comparatively low rate of speed was occasioned by two factors: (1) the slowness with which the eye and hand can work in selecting the proper letter on the keyboard, in noting the cipher letter on the bank of lights, and in writing down the cipher letter; (2) the slowness of the relay referred to above. No doubts are entertained by us, however, in regard to the possibility of increasing the speed to a more satisfactory level without any material change in design of the cryptograph itself. In the first place, speed of operation would certainly increase with practice on the part of an operator, so that in the case of the hand-recording type of machine there is no doubt but that a speed of 50 to 60 characters per minute, equivalent to 10 to 12 five-letter code groups per minute, could be obtained. This is approximately five times faster

than a code book can possibly be handled. In the second place, with the construction of an adapter to be placed in position over the keyboard of a typewriter or of a teletyper, in which case the operator has no writing to do but merely operates the keyboard of the cryptograph, the speed of encipherment could be raised no doubt to 30 - 35 five-letter words per minute, possibly more. Additional details in connection with this adapter will follow.

5. From the cryptographic point of view the present hand-recording model is highly satisfactory. I know of no more secure method. If used between the highest permanent or semipermanent headquarters, it is believed that absolute indecipherability can be accomplished in practical operation; if used between mobile, small headquarters, the degree of security in practical usage will be a function of the pains to which it is thought practicable to go in regard to length and variation of keying tapes. These details can readily be worked out later.

6. The questions which arise in the immediate present are these:

a. How many additional models of the present design should be constructed?
b. Where should they be constructed?
c. Shall development proceed at once with regard to the adapter referred to in paragraph 4?
d. Can funds sufficient for these purposes be made available?

7. In regard to question a, it is recommended that at least two more hand-recording models be constructed without delay, making three machines available for test purposes. Two of these should be sent to this office for cryptographic experimentation and study; the third model should remain at the laboratories for further engineering study.

8. In regard to question b, it is recommended that the two additional models be constructed at the laboratories, rather than by an outside engineering laboratory. In the first place, the desire for secrecy in regard to this machine, at least for the present, dictates the policy that no details should be made available to outside parties. In the second place, the time and cost of construction within the laboratories would be much less than would obtain outside, since very little additional engineering study and experimentation is necessary, all this having now been completed.

9. In regard to question c, it is recommended that the laboratories be directed to initiate a study with regard to the possible development of a suitable adapter to be positioned over the keyboard of either an ordinary typewriter, or of a teletype machine. If feasible, the typing of enciphered and deciphered cryptograms could be accomplished automatically; or, the cryptograph could be used in conjunction with a teletype keyboard so that ultimately it might be possible, without any intermediate steps, to encipher, transmit, receive, decipher and print cryptograms at a high rate of speed. This phase of the development represents only a continuation of the original project as regards cryptographic apparatus.

10. In regard to funds, it is estimated that the entire cost of producing the two additional models recommended in paragraph 7 above, including labor, should not exceed $1000 or $1200, since it is merely a question of duplicating elements already produced, and not of additional engineering or developmental study. As regards the adapter, however, considerable developmental work would be necessary and it is thought by the laboratory personnel that about $5000 will be required for this phase of the project. The question as to whether such a sum can be made available, either in part or in whole, before the beginning of the fiscal year 1933, is left for the consideration of those controlling the disposition of development funds.

11. To summarize, it is desired to indicate that the progress made by the laboratories to date is very satisfactory and gives promise of culminating in the production of a machine that will satisfy every requirement of practicability, speed, accuracy, and security.

William F. Friedman.